INVITATION TO SUBMIT WHITE PAPERS ON DEVELOPING A ROADMAP FOR CYBER SECURITY AND INFORMATION ASSURANCE RESEARCH AND DEVELOPMENT

1. Overview October 31, 2006

This invitation to submit white papers is issued by the Federal government's Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG). The CSIA IWG operates under the auspices of the National Science and Technology Council (NSTC) and was initially established in 2003 as the Critical Information Infrastructure Protection IWG. It was rechartered as the CSIA IWG in 2005 with the role of coordinating policy, programs, and budgets for CSIA research and development (R&D) within the Federal government.

Through this invitation, the Federal government is soliciting input from individuals in academia, industry (including at national laboratories and Federally funded research and development centers [FFRDCs]), and international organizations about the development of a roadmap called for in the *Federal Plan for Cyber Security and Information Assurance Research and Development* released in April 2006 (available online at http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf). Though the call for white papers is primarily intended to solicit viewpoints from outside of the Federal government, the Federal CSIA R&D community is welcome to respond.

The white papers will enable interested stakeholders to provide input that can help shape the future research and development of cyber security and information assurance technologies in the United States. The white papers will also be used to guide future interactions with the respondents and their organizations, including use in selecting persons to invite to anticipated upcoming CSIA IWG-sponsored workshops and other related workshops and events that will be devoted to CSIA R&D roadmap development.

Submission Guidelines: White papers submitted by November 30, 2006 will be used in planning workshops that will be held in 2007. White papers submitted by January 31, 2007 will be used to the greatest extent possible. A white paper should not exceed five pages in length, should be printed in a 12-point font, and should include the author's name, title, affiliation, postal address, e-mail address, and phone number. An appendix of up to ten pages in length may also be included to expand on the white paper such as by providing supplemental explanations, information, or references. Please submit white papers to csia-white-papers@nitrd.gov.

Additional information on the background and scope for this invitation is provided in section 2 below; relevant information from the *Plan* is included in section 3; questions to be addressed in the white papers are in section 4; and the Web site and contact information for this effort are provided in section 5.

2. Background and Scope

In April 2006, the CSIA IWG released a report entitled *Federal Plan for Cyber Security and Information Assurance Research and Development.* In his cover letter transmitting this report, Dr. John H. Marburger, III, Director of the White House Office of Science and Technology Policy (OSTP), who is the President's Science Advisor and chairs the NSTC on behalf of the President, stated that this *Plan* "presents a coordinated interagency framework for addressing critical gaps in current cyber security and information assurance capabilities and technologies," and that he looked forward "to working with Federal agencies and the private sector to develop the research roadmap for the Plan." Subsequently, the June 2006 memorandum on FY 2008 Administration R&D Budget priorities, issued jointly by OSTP and the Office of Management and Budget (OMB), established cyber security as an interagency R&D priority under the

Federal Networking and Information Technology Research and Development (NITRD) Program. The memo stated, "In the area of cyber security, agency plans must be consistent with the 2006 *Federal Plan for Cyber Security and Information Assurance R&D* and should address any relevant gaps identified in the Federal Plan." This call for white papers is a component of the Federal government's efforts to collaborate with the private sector in reviewing and possibly modifying or expanding the *Federal Plan's* list of cyber security and information assurance technical topics and priorities, and to gather additional information in support of the development of a roadmap for cyber security and information assurance R&D.

The scope of the solicited white papers is limited to cyber security and information assurance *research and development*. Other areas, such as policy development (e.g., legislation, regulation, funding), economic issues, operational security approaches and best practices, and Federal agency budgets, also have substantial roles to play in improving cyber security and information assurance but are outside the scope of the solicited white papers.

3. Relevant Information from the *Federal Plan for Cyber Security and Information Assurance Research and Development*

The following information is provided to put the questions in Part 4 in context.

a. Strategic Federal objectives for cyber security and information assurance R&D, derived from a review of policy and legislative drivers and analyses of cyber security threats and infrastructure vulnerabilities as well as Federal agency mission requirements, are presented in Part I of the *Plan* and included in Appendix A of this document.

b. The *Plan* makes ten recommendations about the Federal R&D strategy that is needed to strengthen the cyber security and information assurance of the Nation's IT infrastructure. These recommendations are presented in Part I of the *Plan* and those five that are within the scope of this call for white papers are listed in question eight (Q8) below.

c. As baseline information for future activities, the *Plan* presents a list, developed through a survey and analysis by CSIA agencies, of cyber security and information assurance R&D technical topics, identifying Federal agencies' current top *interagency* technical and funding priorities. The topics are shown in Appendix B of this document. The topics and their categorization should be viewed as a launching point, rather than a definitive or comprehensive list, for analyzing and addressing cyber security and information assurance R&D priorities across the public and private sectors.

4. Questions That the White Papers Are Asked to Address

Authors of white papers are asked to address one or more of the questions listed below. Please limit your discussion to *research and development* as noted in section 2 above.

<u>CSIA R&D Strategic Issues</u>

Q1. The objective of the *Federal Plan* is to foster the development of technological foundations that will enable the creation of a more secure IT infrastructure. What are the most significant technical barriers that will impede attainment of this objective?

Q2. The *Federal Plan* provides an initial step toward creation of a national research and development agenda for strengthening the cyber security and information assurance of the Nation's IT infrastructure. How should the *Plan* be revised or expanded to more comprehensively address the development and implementation of a national research agenda?

CSIA R&D Technical Topics and Priorities listed in the table in Appendix B

Q3. Is the list of topics complete? If not, please identify and describe any omissions. In suggesting a new topic, please follow the template of the *Plan*'s "Technical Perspectives" section, specifically addressing definition, importance, state of the art, and capability gaps.

Q4. The topics reflect Federal agencies' missions and needs. What technical topics are important to academia, industry, national labs, FFRDCs, and international organizations? How are your organization's CSIA priorities established and prioritized?

Q5. Which of the technical topics are common to academia, industry, and government, and are therefore candidates for coordinated approaches? What are possible approaches? What are effective methods for implementing those approaches?

CSIA R&D Roadmap

For the purpose of this call for white papers, a cyber security and information assurance R&D roadmap identifies, completely and with minimal overlap, the R&D needed to realize the strategic Federal objectives referenced in section 3 above. The roadmap also sets forth a timeline, with milestones for performing that R&D, identification of interdependencies among R&D topics, assessment metrics for the R&D results, and a strategy for deploying those results.

Q6. What have been effective roadmapping processes that can be used for the CSIA R&D roadmapping? What are the lessons learned from those processes that can be applied to the CSIA R&D roadmapping effort?

Q7. R&D efforts that will be part of the roadmap include short-term (1 to 3 years), medium-term (3 to 5 years) and long-term (5 years and beyond). How should the technical topics in the roadmap be grouped into short-term, medium-term, and long-term so that effective solutions can be produced?

R&D Recommendations in the *Federal Plan*

Q8. The following *Plan* recommendations have R&D aspects:

- Target Federal R&D investments to strategic cyber security and information assurance needs (*Plan* Recommendation *P*R #1)
- Focus on threats with the greatest potential impact (*P*R #2)
- Build security in from the beginning (*P*R #5)
- Assess security implications of emerging information technologies (*P*R #6)
- Develop and apply new metrics to assess cyber security and information assurance (*P*R #8)

How should each of those recommendations be addressed? How should each be incorporated in the roadmap?

5. Web Site and Contact Information

The CSIA Web site (http://www.nitrd.gov/subcommittee/csia.html) provides information about the CSIA IWG and its activities, including a link to an online copy of the *Plan*, a form for requesting a hard copy, and this call for white papers; the Web site will also provide future information and updates about the roadmap effort.

Please send e-mail to csia-comments@nitrd.gov or call Dr. Ernest McDuffie, CSIA IWG Technical Coordinator, at (703) 292-4504 with any questions about the white papers or to request to be added to the csia-outreach mailing list.

APPENDIX A

Strategic Federal Objectives for Cyber Security and Information Assurance Research and Development

In the *Federal Plan for Cyber Security and Information Assurance Research and Development* released in April 2006 the following strategic Federal objectives (see pages 14 and 15 of the *Plan*) for cyber security and information assurance R&D were derived from a review of policy and legislative drivers and analyses of cyber security threats and infrastructure vulnerabilities as well as Federal agency mission requirements:

1. Support research, development, testing, and evaluation of cyber security and information assurance technologies aimed at preventing, protecting again, detecting, responding to, and recovering from cyber attacks that may have large-scale consequences.
2. Address cyber security and information assurance R&D needs that are unique to critical infrastructures.
3. Develop and accelerate the deployment of new communication protocols that better assure the security of information transmitted over networks.
4. Support the establishment of experimental environments such as testbeds that allow government, academic, and industry researchers to conduct a broad range of cyber security and information assurance development and assessment activities.
5. Provide a foundation for the long-term goal of economically informed, risk-based cyber security and information assurance decision making.
6. Provide novel and next-generation secure information technology concepts and architectures through long-term research.
7. Facilitate technology transition and diffusion of Federally-funded R&D results into commercial products and services and private-sector use.

APPENDIX B

From pages 18 and 19 of the *Federal Plan for Cyber Security and Information Assurance Research and Development* report by the Interagency Working Group on Cyber Security and Information Assurance published April of 2006.

TABLE 1

Top Technical and Funding Priorities

Federal Cyber Security and Information Assurance R&D

CSIA R&D AREAS Categories and Technical Topics	TOP PRIORITIES Technical	 Funding
1. Functional Cyber Security and Information Assurance		
1.1 Authentication, authorization, and trust management	✓	✓
1.2 Access control and privilege management	✓	✓
1.3 Attack protection, prevention, and preemption	✓	✓
1.4 Large-scale cyber situational awareness	✓	
1.5 Automated attack detection, warning, and response		✓
1.6 Insider threat detection and mitigation		
1.7 Detection of hidden information and covert information flows		
1.8 Recovery and reconstitution		
1.9 Forensics, traceback, and attribution		
2. Securing the Infrastructure		
2.1 Secure Domain Name System		
2.2 Secure routing protocols		
2.3 IPv6, IPsec, and other Internet protocols		
2.4 Secure process control systems	✓	
3. Domain-Specific Security		
3.1 Wireless security	✓	✓
3.2 Secure radio frequency identification		
3.3 Security of converged networks and heterogeneous traffic	✓	
3.4 Next-generation priority services		
4. Cyber Security and Information Assurance Characterization and Assessment		
4.1 Software quality assessment and fault characterization		✓
4.2 Detection of vulnerabilities and malicious code	✓	
4.3 Standards		
4.4 Metrics		
4.5 Software testing and assessment tools	✓	✓
4.6 Risk-based decision making		
4.7 Critical infrastructure dependencies and interdependencies		

Top Technical and Funding Priorities (continued)

CSIA R&D AREAS Categories and Technical Topics	TOP PRIORITIES Technical	 Funding
5. Foundations for Cyber Security and Information Assurance		
5.1 Hardware and firmware security		
5.2 Secure operating systems		
5.3 Security-centric programming languages		
5.4 Security technology and policy management methods and policy specification languages		
5.5 Information provenance		
5.6 Information integrity		
5.7 Cryptography		✓
5.8 Multi-level security		
5.9 Secure software engineering		✓
5.10 Fault-tolerant and resilient systems		
5.11 Integrated, enterprise-wide security monitoring and management		
5.12 Analytical techniques for security across the IT systems engineering life cycle		✓
6. Enabling Technologies for Cyber Security and Information Assurance R&D		
6.1 Cyber security and information assurance R&D testbeds		✓
6.2 IT system modeling, simulation, and visualization	✓	
6.3 Internet modeling, simulation, and visualization		
6.4 Network mapping		
6.5 Red teaming		
7. Advanced and Next-Generation Systems and Architectures		
7.1 Trusted computing base architectures		✓
7.2 Inherently secure, high-assurance, and provably secure systems and architectures	✓	
7.3 Composable and scalable secure systems	✓	
7.4 Autonomic systems		✓
7.5 Architectures for next-generation Internet infrastructure	✓	
7.6 Quantum cryptography		
8. Social Dimensions of Cyber Security and Information Assurance		
8.1 Trust in the Internet		
8.2 Privacy	✓	